4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/798,079	03/11/2004	Aaron Charles Newman	AS2	5342

7590 03/06/2007

Peter S. Canelias
Law Offices of Peter S. Canelias
Suite 2148
420 Lexington Avenue
New York, NY 10170

EXAMINER	
KIM, PAUL	
ART UNIT	**PAPER NUMBER**
2161	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/798,079	NEWMAN ET AL.	
	Examiner	Art Unit	
	Paul Kim	2161	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 December 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *22-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *22-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/11/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is responsive to the following communication: Amendment filed on 8 December 2006.

2. Claims 1-88 are pending and present for examination. Claims 1, 7, 14, 22, 31, 36, 40, 42, 50, 53, 54, 60, and 64 are independent.

Election/Restrictions

3. Applicant's election with traverse of Group 4, claims 22-30, in the reply filed on 8 December 2006 is acknowledged. The traversal is on the ground(s) that "the examiner consider class 726 subclass 22" which would remove "any burden on the examiner" (See Amendment, page 24). This is not found persuasive because regardless of the classification of the claimed species, the claimed invention still comprises of multiple preferred embodiments.

The requirement is still deemed proper and is therefore made FINAL.

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on 11 March 2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. **Claims 22-30** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed toward "a method for detecting unauthorized

activity," and are non-statutory because they do not encompass tangible subject matter and/or embodiments which fall within a statutory category.

The claims make no mention of a tangible medium wherein existing code may be processed to perform the recited steps in the claims. See State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. MPEP 2106. "The claimed invention as a whole must accomplish a practical application. That is, it must produce a 'useful, concrete and tangible result' " (emphasis added).

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. **Claims 22-23** are rejected under 35 U.S.C. 102(b) as being anticipated by Bapat et al (U.S. Patent No. 6,038,563, hereinafter referred to as BAPAT), filed on 25 March 1998, and issued on 14 March 2000.

9. **As per independent claim 22,** BAPAT teaches:

A method for detecting unauthorized activity in a database application, the method comprising:

monitoring for SQL statements executable in said database application and intended to perform activities not authorized by an SQL source {See BAPAT, Abstract, wherein this reads over "[a] user access request to access management information in the database is intercepted, and the access control procedure is invoked when the user access request is a select statement"; and C18:L19-27, wherein this reads over "every user query for information from the tables in the DBMS is checked by the SQL engine 286 against the access rights established by the access privileges module"};

actuating each discrete database event {See BAPAT, C18:L24-27, wherein this reads over "[u]ser queries requesting information from tables to which the user does not have access rights are rejected by the SQL engine"};

analyzing each event against a pre-defined set of detection rules {See BAPAT, C17:L15-19, wherein this reads over "a Security Alarm log 293 that is separate from the security audit trail 192, where security alarms are generated and stored in the log only when there is a denial of object access"}.

10. **As per dependent claim 23,** BAPAT teaches:

> The method according to claim 22, wherein said unauthorized activity is accessing data for which said SQL source has not been granted privileges {See BAPAT, C18:L24-27, wherein this reads over "[u]ser queries requesting information from tables to which the user does not have access rights are rejected by the SQL engine"}.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 24 and 26-30** are rejected under 35 U.S.C. 103(a) as being unpatentable over BAPAT as applied to claims 22 and 23 above, and further in view of Rowland (U.S. Patent No. 6,405,318, hereinafter referred to as ROWLAND), filed on 12 March 1999, and issued on 11 June 2002.

13. **As per dependent claim 24,** while BAPAT fails to expressly disclose a method "wherein said unauthorized activity is accessing data not using an authorized method," ROWLAND discloses a method wherein "[t]he user login is checked to determined if there are multiple concurrent logins for the same user" {See ROWLAND, C5:L10-20}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND. That is, the inclusion of the disclosed invention in ROWLAND would provide a means for checking for multiple concurrent logins (i.e. an unauthorized method of access).

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

14. **As per dependent claim 26,** while BAPAT fails to expressly disclose a method "wherein said unauthorized activity is interfering with auditing settings," ROWLAND discloses a method wherein "[i]f a suspicious directory name is found 68, the control function is notified 55" {See ROWLAND, C6:L4-11}.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

15. **As per dependent claim 27,** while BAPAT fails to expressly disclose a method "wherein said unauthorized activity is interfering with audit records," ROWLAND discloses a method wherein "[t]he system checks to determined if the system audit records have been altered or are missing" {See ROWLAND, C6:L4-11}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

16. **As per dependent claim 28,** while BAPAT fails to expressly disclose a method "wherein said unauthorized activity is modifying configuration settings," ROWLAND discloses a method wherein a determination is made as to whether "the user's home directory contains one or more suspicious directories" {See ROWLAND, C5:L61-63}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

17. **As per dependent claim 29,** while BAPAT fails to expressly disclose a method "wherein said unauthorized activity is modifying security settings," ROWLAND discloses a method wherein "[t]he system examines the rhost file and other system authentication files to determine if dangerous security modifications to the host file have occurred" {See ROWLAND, C5:L53-56}. Therefore, it would have been

obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

18. **As per dependent claim 30,** while BAPAT fails to expressly disclose a method "wherein said unauthorized activity is a use of an unauthorized tool to attempt to access said database application," ROWLAND discloses a method wherein "[t]he port scan detector of the present invention alerts administrators that a person is actively looking for services on their host" using "a program that may either connect to all ports on the remote machine or deliberately pick one or more ports to search" {See ROWLAND, C6:36-67}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

19. **Claim 25** is rejected under 35 U.S.C. 103(a) as being unpatentable over BAPAT as applied to claims 22 and 23 above, further in view of ROWLAND, as applied to claims 24 and 26-40 above, and further in view of Official Notice.

20. **As per dependent claim 25,** while BAPAT and ROWLAND fail to expressly disclose a method "wherein said unauthorized activity is accessing data in a data dictionary not using an authorized method," the Examiner takes Official Notice that it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide security checks for unauthorized activity in a data dictionary.

Conclusion

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul Kim whose telephone number is (571) 272-2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Apu Mofiz can be reached on (571) 272-4080. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Paul Kim
Patent Examiner, Art Unit 2161
TECH Center 2100